Structure de groupe et d'anneau

Table des matières

1 Loi de composition interne. 2
1.1 Définition . . . 2
1.2 Commutativité et associativité . . . 3
1.3 Élément neutre . . . 4
1.4 Symétrique . . . 4
1.5 Distributivité d'une loi par rapport à une autre . . . 5
1.6 Partie stable par une loi . . . 6

2 Groupe 6
2.1 Définition . . . 6
2.2 Permutation et groupe symétrique . . . 7
2.3 Sous-groupe . . . 7
2.4 Groupe produit . . . 9

3 Anneau 9
3.1 Définition . . . 9
3.2 Anneau intègre . . . 10
3.3 Groupe des inversibles d'un anneau . . . 10
3.4 Sous-anneau . . . 11
3.5 Corps . . . 12

Introduction

Tout le monde associe au mot algèbre le mot calcul. L'algèbre classique consiste ainsi à calculer sur des nombres. Le développement de l'algèbre au XIX^e et au XX^e siècle a obligé les mathématiciens à calculer sur des objets mathématiques variés et à isoler les situations qu'on rencontre constamment. On a ainsi été conduit aux notions de groupe, d'anneau et de corps. La première situation s'est rencontré en Géométrie avec le groupe des transformations (translation, rotation, symétries, homothétie), en Arithmétique avec Gauss et en Algèbre avec Galois dans l'étude des équations algébriques. C'est ainsi que la notion de groupe, qu'Arthur Cayley a le premier défini, est aussi importante que la notion de fonction ou d'ensemble. Quant aux notions d'anneau et de corps, on les utilise dans toutes les branches des mathématiques car elles permettent l'emploi d'une terminologie commode.

1 Loi de composition interne.

1.1 Définition

Définition 1 : Soit E un ensemble.

La loi $*$ est une loi de composition interne sur E si, et seulement si :

$$\forall x, y \in E, \quad x * y \in E$$

L'ensemble E muni de la loi de composition interne $*$, $(E, *)$, est appelé magma

Remarque : Une loi de composition interne est ce que l'on nomme usuellement une opération. Dans l'ensemble $\mathbb{N}$, on définit ainsi deux lois de composition interne + et $\times$ qui sont respectivement l'addition et la multiplication.

Un magma est la structure primitive qui permet d'effectuer des calculs.

Exemples :

- $(\mathbb{N}, +)$ et $(\mathbb{N}, \times)$ sont des magmas.
- $(\mathscr{M}_n(\mathbb{K}), +)$ et $(\mathscr{M}_n(\mathbb{K}), \times)$ sont des magmas car la somme ou le produit de deux matrices carrées de taille n est une matrice carrée de taille n.
- L'ensemble des isométries du plan muni de la loi $\circ$ est un magma. En effet la composition de deux isométries est une isométrie.
- L'ensemble des parties d'un ensemble E, $\mathscr{P}(E)$, muni de la loi $\cup$ ou $\cap$ est un magma car l'union ou l'intersection d'une partie de E est encore une partie de E

Remarque : Lorsque l'ensemble E est fini, on représente la loi $*$ par un tableau.

- Pour un ensemble $E = \{a, b, c\}$ muni de la loi $*$:

$*$	a	b	c
a	$a*a$	$a*b$	$a*c$
b	$b*a$	$b*b$	$b*c$
c	$c*a$	$c*b$	$a*c$

- Pour l'ensemble $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$, des restes de la division d'un entier par 4, on définit alors les tables d'addition et de multiplication.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1.2 Commutativité et associativité

Définition 2 : Soit $(E,*)$ un magma.

- $(E,*)$ est associatif si : $\forall a,b,c \in E,\ (a*b)*c = a*(b*c) = a*b*c$
- On dit que $(E,*)$ est commutatif si : $\forall a,b \in E,\ a*b = b*a$

Remarque :

- L'associativité permet d'enlever les parenthèse sans changer le résultat.
- L'associativité permet la définition de la « puissance » d'un élément a de E pour la loi $*$: $\overbrace{a*a\cdots*a}^{n \text{ fois}} = a^n$.

  Lorsqu'on utilise la loi $+$ on adopte la convention suivante faisant référence à l'addition des entiers :

  $a+a+\cdots+a = na$, on parle alors de multiple plutôt que de puissance.
- Certaines lois ne sont pas associatives c'est le cas du produit vectoriel « $\wedge$ » dans l'espace (au sens usuel du terme) ou la soustraction dans l'ensemble $\mathbb{Z}$, en effet :

$$\left.\begin{array}{l}(3-2)-1 = 1-1 = 0\\ 3-(2-1) = 3-1 = 2\end{array}\right\} \Rightarrow (3-2)-1 \neq 3-(2-1)$$

- Certaines lois ne sont pas commutatives c'est le cas par exemple de la composition des fonctions de E dans E. Si l'on prend deux fonctions constantes :

  $\forall x \in E,\ f(x) = a$ et $g(x) = b$ avec $a \neq b$ alors :

$$\forall x \in E,\quad \left.\begin{array}{l}g\circ f(x) = g(a) = b\\ f\circ g(x) = f(b) = a\end{array}\right\} \Rightarrow g\circ f \neq f\circ g$$

Exemples :

- $(\mathbb{N},+)$, $(\mathbb{N},\times)$, $(\mathbb{R},+)$ et $(\mathbb{R},\times)$ sont commutatifs et associatifs.
- $(\mathscr{M}_n(\mathbb{K}),+)$ est commutatif et associatif.
- $(\mathscr{M}_n(\mathbb{K}),\times)$ est associatif mais pas commutatif.
- $(\mathscr{P}(E),\cup)$ et $(\mathscr{P}(E),\cap)$ sont associatifs et commutatifs.

1.3 Élément neutre

Définition 3 : Soit $(E, *)$ un magma. On dit que e est un élément neutre de E pour $*$ si :

$$\forall x \in E, \quad x * e = e * x = x$$

Si cet élément neutre existe, il est unique

Démonstration : Soient e et e' deux éléments neutres de E pour $*$ alors on a :

$$e' \overset{e \text{ neutre}}{=} e * e' \overset{e' \text{ neutre}}{=} e$$

Exemples :

- L'élément neutre de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ pour l'addition $+$ est 0.
- L'élément neutre de $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ pour la multiplication $\times$ est 1
- L'élément neutre de $\mathscr{P}(E)$, pour l'union $\cup$ est $\varnothing$
- L'élément neutre de $\mathscr{P}(E)$, pour l'intersection $\cap$ est E
- L'élément neutre de $\mathscr{M}_n(\mathbb{K})$ pour la multiplication $\times$ est I_n
- L'élément neutre de E^E, pour la composition $\circ$ est Id_E

Remarque :

- Si la loi $*$ n'est pas commutative, E peut ne pas avoir d'élément neutre mais avoir un élément neutre à droite et un élément neutre à gauche.
- Dans $(E, *)$, par convention on notera $x^0 = e$.
  - Pour une loi additive +, on écrira $0x = 0$ ou $0x = 0_E$
  - Dans $\mathscr{M}_n(\mathbb{K})$, on écrira $M^0 = I_n$.
  - Dans E^E, on écrira $f^0 = \mathrm{Id}_E$

1.4 Symétrique

Définition 4 : Soit $(E, *)$ possédant un élément neutre e. On dit que x admet un symétrique pour $*$ s'il existe $x' \in E$ tel que : $x * x' = x' * x = e$

Si $(E, *)$ est **associatif** alors le symétrique d'un élément x de E est unique.

Démonstration : Soit $(E, *)$ un magma associatif d'élément neutre e et x qui admet deux symétriques x'_1 et x'_1. On a alors

$$x'_2 = x'_2 * e \overset{x'_1 \text{ sym.}}{=} x'_2 * (x * x'_1) \overset{\text{associativité}}{=} (x'_2 * x) * x'_1 \overset{x'_2 \text{ sym.}}{=} e * x'_1 = x'_1$$

Remarque :

- Le symétrique de x dans une loi additive, s'appelle l'**opposé** de x noté $(-x)$.
- Le symétrique de x dans une loi multiplicative s'appelle l'**inverse** de x noté x^{-1}
- Le symétrique de f pour la loi de composition $\circ$ dans E^E s'appelle la réciproque de f noté f^{-1}

Le symétrique de x pour la loi $*$ dans la suite du chapitre, sera appelé l'inverse et sera noté x^{-1}

Propriété 1 : Soit $(E,*)$ un magma associatif d'élément neutre e. Soit x, y et z trois éléments de E.

- **Simplification** avec x inversible : $\begin{cases} \text{Si } x*y = x*z \Rightarrow y = z \\ \text{Si } y*x = z*x \Rightarrow y = z \end{cases}$
- **Inversibilité du produit** : Si x et y sont inversible alors $x*y$ est inversible et $(x*y)^{-1} = y^{-1}*x^{-1}$
- **Puissances négatives** :
  $\forall n \in \mathbb{N}$, x inversible $\Rightarrow$ x^n est inversible et $(x^n)^{-1} = x^{-n}$
- **Inverse de l'inverse** : Si x est inversible alors x^{-1} est inversible et $(x^{-1})^{-1} = x$

Démonstration :

- Simplification : (à gauche) : (H) : $x*y = x*z$
  $y = e*y = (x^{-1}*x)*y = x^{-1}*(x*y) \overset{(H)}{=} x^{-1}*(x*z) = (x^{-1}*x)*z = e*z = z$
- Inversibilité du produit :
  $$(x*y)*(y^{-1}*x^{-1}) = x*(y*y^{-1})*x^{-1} = x*e*x^{-1} = x*x^{-1} = e$$
  ⚠ Si la loi $*$ n'est pas commutative faire attention à l'ordre $(x*y) = y^{-1}*x^{-1}$
- Puissance négative : récurrence sur $\mathbb{N}$. Pour l'hérédité HR : $(x^n)^{-1} = (x^{-1})^n$
  $$(x^{n+1})^{-1} = (x*x^n)^{-1} \overset{\text{par produit}}{=} (x^n)^{-1}*x^{-1} \overset{\text{HR}}{=} (x^{-1})^n*x^{-1} = (x^{-1})^{n+1}$$
- Pour l'inverse de l'inverse : immédiat du fait de la symétrie de la définition.

Exemples :

- $(\mathbb{N},+)$ ne possède qu'un seul nombre opposé l'élément neutre 0.
- Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ tout nombre possède un opposé.
- $(\mathbb{Z},\times)$ ne possède que deux nombres inversibles 1 et -1.
- Dans $(\mathbb{Q}^*,+)$, $(\mathbb{R}^*,+)$, $(\mathbb{C}^*,+)$ tout nombre possède un inverse.
- Dans $(\mathscr{M}_n(\mathbb{K}),+)$ toute matrice possède un opposé.
- Dans $(\mathrm{GL}_n(\mathbb{K}),\times)$ toute matrice est inversible.
- Dans $(E^E,\circ)$, seule les fonctions bijectives admettent une réciproque.

1.5 Distributivité d'une loi par rapport à une autre

Définition 5 : Soit un ensemble E muni de deux lois de compositions internes $*$ et $\circ$. On dit que $*$ est distributive par rapport à $\circ$ si :

$$\forall x,y,z \in E, \quad x*(y\circ z) = (x*y)\circ(x*z) \quad \text{et} \quad (y\circ z)*x = (y*x)\circ(z*x)$$

Exemple : Dans $\mathscr{P}(E)$ les lois commutatives intersection $\cap$ et union $\cup$ sont distributives l'une par rapport à l'autre.

$$\text{distributivité de } \cap \text{ par rapport à } \cup : \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$\text{distributivité de } \cup \text{ par rapport à } \cap : \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

1.6 Partie stable par une loi

Définition 6 : Soient $(E, *)$ un magma et A une partie de E. On dit que A est stable par $*$ si :

$$\forall x, y \in A, \quad x * y \in A$$

$(A, *)$ est alors un magma.

Exemples :

- Dans $(\mathbb{C}, +)$, l'ensemble $i\mathbb{R}$ des imaginaires purs est stable pour l'addition.
- Dans $(\mathbb{C}, \times)$, l'ensemble $i\mathbb{R}$ des imaginaires purs n'est pas stable pour la multiplication : $2i \times 3i = -6 \notin i\mathbb{R}$

2 Groupe

2.1 Définition

Définition 7 : On dit que le magma $(G, *)$ est un groupe si :

- $*$ est associative.
- G possède un élément neutre e.
- Tout élément de G est inversible

Si $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou abélien

Remarque : Pour simplifier la rédaction on dira tout simplement « soit un groupe G » au lieu de dire « soit un groupe $(G, *)$ ». Dans le même esprit, on utilisera la notation multiplicative au lieu de la loi $*$. On écrira par exemple xy pour $x * y$. On notera parfois 1_G l'élément neutre.

Dans G tout élément est inversible, on a alors : $xy = xz \overset{\times x^{-1}}{\Rightarrow} y = z$.

Exemples :

- Groupes commutatifs
  - $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$
  - $(\mathbb{Z}^*, \times)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$
  - $(\mathscr{M}(\mathbb{K}), +)$
- Groupes non commutatifs
  - $(\mathrm{GL}_n(\mathbb{K}), \times)$: l'ensemble des matrices inversibles d'ordre n
  - $(i, \circ)$: ensemble des isométries du plan.

2.2 Permutation et groupe symétrique

Définition 8 : Soit E un ensemble non vide.

- On appelle permutation de E toute bijection de E sur E
- On appelle groupe symétrique de E l'ensemble des permutation de E, noté S_E. Le magma $(S_E, \circ)$ est un groupe d'élément neutre Id_E.

Démonstration : Montrons que $(S_E, \circ)$ est un groupe.

- S_E est stable par $\circ$ car la composée de deux bijections est une bijection.
- $\circ$ est associative.
- $\mathrm{Id}_E \in S_E$ est l'élément neutre.
- Toute bijection est inversible.

2.3 Sous-groupe

Définition 9 : Soient G un groupe et H une partie stable de G. On dit que H est un sous-groupe de G si H est un groupe pour la loi de G.

Théorème 1 : Soient G un groupe et H une partie de G.

$$H \text{ sous-groupe de } G \Leftrightarrow \begin{cases} 1_G \in H \\ \forall x, y \in H, \ \ xy^{-1} \in H \end{cases}$$

Remarque : Pour montrer qu'un ensemble E est un groupe, une méthode très efficace consiste à montrer qu'il est le sous-groupe d'un groupe qui le contient.

Démonstration : Par double implication

- Si H est un sous-groupe de G alors
  - $H \subset G$ et contient l'élément neutre de G.
  - H est stable et tout élément de H est inversible donc : $\forall x, y \in H, \ \ xy^{-1} \in H$.
- Réciproquement, $1_G \in H$ et $\forall x, y \in H, \ \ xy^{-1} \in H$ (1)
  - H n'est pas vide car contient 1_G. De plus $\forall y \in H, \ \overbrace{1_G y^{-1} = y^{-1} \in H}^{\text{d'après (1)}}$. H est stable par passage à l'inverse.
  - H est stable par passage à l'inverse et d'après (1), $\forall x, y \in H, \ \ y^{-1} \in H \ \Rightarrow \ x(y^{-1})^{-1} = xy \in H$. H est donc stable.
  - L'associativité se transmet à H car $H \subset G$

Exemples :

- G et $\{1_G\}$ sont des sous-groupes de G.

- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ qui est un sous-groupe de $(\mathbb{R}, +)$ qui est un sous-groupe de $(\mathbb{C}, +)$.
- $\mathbb{U}$ ensemble des complexes de module 1 : $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$.
  $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$: en effet :
  - $\mathbb{U} \subset \mathbb{C}$
  - $1 \in \mathbb{U}$ car $|1| = 1$.
  - $\forall z, z' \in \mathbb{U}, \quad |z\,(z')^{-1}| = |z| \times |(z')^{-1}| = |z| \times \left|\dfrac{1}{z'}\right| = \dfrac{|z|}{|z'|} = \dfrac{1}{1} = 1 \in \mathbb{U}$
- $\mathbb{U}_n$ ensemble des racines n-ième de l'unité dans $\mathbb{C}$. $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$.
  $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$: en effet :
  - $\mathbb{U}_n \subset \mathbb{U}$ car $|z^n| = |z|^n = 1 \ \Rightarrow |z| = 1$
  - $1 \in \mathbb{U}_n$ car $1^n = 1$.
  - $\forall z, z' \in \mathbb{U}_n, \quad \left[z\,(z')^{-1}\right]^n = \left(\dfrac{z}{z'}\right)^n = \dfrac{z^n}{(z')^n} = \dfrac{1}{1} = 1 \in \mathbb{U}_n$
- $n\mathbb{Z}$ ensemble des multiples de $n \in \mathbb{N}^*$: $n\mathbb{Z} = \{kn,\ k \in \mathbb{Z}\}$
  $(n\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$. ⚠ notation additive.
  - $n\mathbb{Z} \subset \mathbb{Z}$
  - $0 \in nZ$ car 0 est un multiple de n
  - $\forall x, y \in n\mathbb{Z}, \quad x + (-y) = kn + (-k'n) = -kk'\,n \in n\mathbb{Z}$
- $H = 5\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$.
  H n'est pas stable. Contre-exemple : $5 \in H$ et $8 \in H$ mais $5 + 8 = 13 \notin H$
- Soit $H = \{2^n,\ n \in \mathbb{Z}\}$.
  H est le plus petit sous-groupe de $(\mathbb{R}^*, \times)$ contenant $\{2\}$.
  1) Montrons que $(H, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$
     - $H \subset \mathbb{R}^*$
     - $1 \in H$ car $2^0 = 1 \in H$
     - $\forall x, y \in H,\ xy^{-1} = 2^n \times (2^{n'})^{-1} = \dfrac{2^n}{2^{n'}} = 2^{n-n'} \in H$
  2) Soit H' un sous-groupe de $(\mathbb{R}^*, \times)$ contenant $\{2\}$
     - $1 \in H'$ donc $2^0 = 1 \in H'$.
     - Soit $n \in \mathbb{N}^*$, H' est stable pour $\times$, donc $\underbrace{2 \times 2 \times \cdots \times 2}_{n \text{ fois}} = 2^n \in H'$

       par inversibilité $(2^n)^{-1} = 2^{-n} \in H'$

     Donc $H' \subset H$. Donc H plus petit sous-groupe de $(\mathbb{R}^*, \times)$ contenant $\{2\}$.

  On dit que H est le sous-groupe de $(\mathbb{R}^*, \times)$ **engendré** par $\{2\}$
- Soient un ensemble E et $x \in E$.
  On définit $\mathrm{Stab}(x)$ l'ensemble des bijections de E sur E qui rend x invariant :
  $$\mathrm{Stab}(x) = \{\sigma \in S_E,\ \sigma(x) = x\}$$
  $(\mathrm{Stab}(x), \circ)$ est un sous-groupe de $(S_E, \circ)$

- $\mathrm{Stab}(x) \subset S_E$.
- $\mathrm{Id}_E \in \mathrm{Stab}(x)$ car Id_E est l'élément neutre de S_E et $\mathrm{Id}_E(x) = x$
- $\forall \sigma_1, \sigma_2 \in \mathrm{Stab}(x)$, $\sigma_1 \circ (\sigma_2)^{-1} \in \mathrm{Stab}(x)$ car :
  $\sigma_2(x) = x \Rightarrow (\sigma_2)^{-1}(x) = x$ et $\sigma_1 \circ (\sigma_2)^{-1}(x) = \sigma_1(x) = x$

2.4 Groupe produit

Définition 10 : Soient G_1 et G_2 deux groupes.

On définit la loi de composition interne sur l'ensemble $G_1 \times G_2$ telle que :
$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2, \quad (x_1, x_2)(y_1, y_2) = (x_1 y_1 \ , \ x_2 y_2)$.

Muni de cette loi, $G_1 \times G_2$ est un groupe d'élément neutre $(1_{G_1}, 1_{G_2})$ appelé groupe produit de G_1 et G_2.

On généralise cette construction au produit d'une famille de groupes.

Exemple : Le produit de (x, u) et (x', u') dans le groupe $(\mathbb{R}, +) \times (\mathbb{U}, \times)$ est tel que : $(x, u)(x', u') = (x + x' \ , \ uu')$

3 Anneau

3.1 Définition

Définition 11 : Soient A un ensemble et deux lois $+$ et $\times$ de composition internes sur A.

On dit que $(A, +, \times)$ est un anneau si :

- $(A, +)$ est un groupe commutatif dont l'élément neutre est noté 0_A ou 0.
- $(A, \times)$ est un magma associatif possédant un élément neutre noté 1_A ou 1
- la multiplication $\times$ est distributive par rapport à l'addition $+$.

Si $(A, \times)$ est commutatif, on dit que l'anneau $(A, +, \times)$ est commutatif.

Remarque : Comme pour un anneau, on prend $+$ comme 1re loi et $\times$ comme 2e loi, on écrira tout simplement soit A un anneau.

Rappelons que : $n \in \mathbb{N}$, $a \in A$, $na = \underbrace{a + a + \cdots + a}_{n \text{ fois}}$ et $a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}$

Comme $(A, +)$ groupe commutatif : $n \in \mathbb{N}$, $n(-a) = \underbrace{(-a) + \cdots + (-a)}_{n \text{ fois}} = -na$

Exemples :

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{K}[X], +, \times)$ l'ensemble des polynômes sur $\mathbb{K}$ est un anneau commutatif.
- $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau non commutatif.

Théorème 2 : Règle de calcul dans un anneau.

Soient A un anneau et $a, b \in A$, on a les relations suivantes :

- $0 \times 1_A = 1_A \times 0 = 0_A$
- $\forall n \in \mathbb{Z} : \quad n(ab) = (na)b = a(nb)$
- $(-a)(-b) = ab$ donc $(-1_A)^2 = 1_A$
- $\forall n \in \mathbb{N}$ et si A anneau **commutatif** :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \quad \text{et} \quad a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}$$

Remarque : Si A est un anneau commutatif, la seule chose qu'on ne puisse pas faire c'est de « diviser ».

3.2 Anneau intègre

Définition 12 : Soit A un anneau. On dit que A est intègre si :

$$\forall a, b \in A, \quad ab = 0 \quad \Rightarrow \quad a = 0 \text{ ou } b = 0$$

Exemple : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux intègres

Remarque : Il existe des anneaux qui ne sont pas intègres. On dit alors que l'anneau admet des « diviseurs de 0 ». Par exemple :

- L'anneau $\mathbb{Z}/6\mathbb{Z}$ ensemble des restes de la division par 6 : $2 \times 3 \equiv 6 \equiv 0\ [6]$
- L'anneau $\mathcal{M}_n(\mathbb{K})$: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Par contre l'anneau des polynômes $\mathbb{K}[X]$ est intègre.

3.3 Groupe des inversibles d'un anneau

Théorème 3 : Soit A un anneau.

L'ensemble des éléments inversibles de A est un groupe pour la loi $\times$ noté $U(A)$.

Démonstration :

- $U(A)$ stable car le produit de deux inversibles est inversible : $(xy)^{-1} = y^{-1}x^{-1}$
- $1_A \in U(A)$ car 1_A est inversible : $1_A \times 1_A = 1_A$.
- L'associativité se transmet de A à $U(A)$
- Par définition tout élément de $U(A)$ est inversible

Exemples :

- $U(\mathbb{Z}) = \{-1, 1\}$, et $U(\mathcal{M}_n(\mathbb{K})) = \mathrm{GL}_n(\mathbb{K})$

- Montrons que $U(\mathbb{Z}/n\mathbb{Z}) = \{a \in \mathbb{Z}/n\mathbb{Z},\ \text{pgcd}(a,n) = 1\}$

  $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$ est l'ensemble des restes dans la division par $n \geqslant 2$

  Soit $a, b \in \mathbb{Z}/n\mathbb{Z}$ alors

  $ab \equiv 1\ [n] \overset{k\in\mathbb{Z}}{\Leftrightarrow} ab = 1 + kn \Leftrightarrow ab + (-k)n = 1 \overset{\text{Bézout}}{\Leftrightarrow} \text{pgcd}(a,n) = 1$

3.4 Sous-anneau

Définition 13 : Soient A un anneau et B une partie stable par addition et produit. On dit que B est un sous-anneau de A si B contient 1_A et si B est un anneau pour les lois de A.

Exemple : $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, un sous-anneau de $\mathbb{R}$ qui est un sous-anneau de $\mathbb{C}$.

Théorème 4 : Soient A un anneau et B une partie de A.

$$B \text{ sous-anneau de } A \Leftrightarrow \begin{cases} 1_A \in B \\ \forall x, y \in B,\ x - y \in B \\ \forall x, y \in B,\ xy \in B \end{cases}$$

Remarque : Pour montrer que B est un sous-anneau, on doit montrer que B possède l'élément neutre de la multiplication et qu'il soit stable par différence ($x - y$ est la traduction pour la loi $+$ de xy^{-1} pour la loi $\times$) et stable par produit.

Exemples :

1) L'ensemble des entiers de Gauss, $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est un sous anneau de $\mathbb{C}$, car
   - $\mathbb{Z}[i] \in \mathbb{C}$
   - $1 + 0\,i = 1$ donc $1 \in \mathbb{Z}[i]$
   - $\forall x, y \in B,\ x - y = (a + ib) - (a' + ib') = (\underbrace{a - a'}_{\in\mathbb{Z}}) + i(\underbrace{b - b'}_{\in\mathbb{Z}}) \in \mathbb{Z}[i]$
   - $\forall x, y \in B,\ xy = (a + ib)(a' + ib') = (\underbrace{aa' - bb'}_{\in\mathbb{Z}}) + i(\underbrace{ab' + ba'}_{\in\mathbb{Z}}) \in \mathbb{Z}[i]$

2) Soit a un élément d'un anneau A.
   L'ensemble $\mathbb{Z}(a) = \{x \in A,\ xa = ax\}$ des éléments de A qui commutent avec a est un sous-anneau de A car :
   - $1_A\, a = a\, 1_A$ donc $1_A \in \mathbb{Z}(a)$
   - $\forall x, y \in \mathbb{Z}(a),\ x - y \in \mathbb{Z}(a)$ car

     $(x - y)a = xa + (-y)a = xa - ya \overset{x,y\in\mathbb{Z}(a)}{=} ax - ay = ax + a(-y) = a(x - y)$

- $\forall x, y \in \mathbb{Z}(a),\ \ xy \in \mathbb{Z}(a)$ car
  $(xy)a = x(ya) \overset{y\in\mathbb{Z}(a)}{=} x(ay) = (xa)y \overset{x\in\mathbb{Z}(a)}{=} (ax)y = a(xy)$

3) L'ensemble $n\mathbb{Z}$ des multiple de n, avec $n \geqslant 2$, n'est pas un sous-anneau de $\mathbb{Z}$ car il ne possède pas l'élément neutre multiplicatif 1.

3.5 Corps

Définition 14 : On appelle corps tout anneau commutatif dans lequel tout élément, **non nul**, est inversible.

Remarque : Pour certains auteurs, la commutativité de la 2e loi n'est pas nécessaire. On parle alors de corps et de corps commutatif.

La différence essentiel entre anneau et corps, c'est que dans un corps l'on peut « diviser », sauf par 0, car tout élément non nul est inversible.

Tout corps est intègre car $(a \neq 0_A \text{ et } ab = 0_A) \overset{\times a^{-1}}{\Rightarrow} b = 0$.

Exemples :

- $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps mais pas $\mathbb{Z}$ qui n'admet que -1 et 1 comme inversibles.
- L'ensemble des fractions rationnelles, $\mathbb{K}(X)$ est un corps.
- L'ensemble des matrices inversibles d'ordre n, $\mathrm{GL}_n(\mathbb{K})$ est un « corps non commutatif ».
- L'ensemble des restes dans la division par p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps car

  Les éléments a de $(\mathbb{Z}/p\mathbb{Z})$ sont inversibles ssi $\mathrm{pgcd}(a, p) = 1$.

  Comme p est premier et comme tout élément a non nul de $\mathbb{Z}/p\mathbb{Z}$ sont tels que $1 \leqslant a \leqslant p-1$, alors $\mathrm{pgcd}(a, p) = 1$

- L'ensemble de dislocation de X^2+1, $\mathbb{Q}(i) = \{a + ib,\ \ a, b \in Q\}$ est un corps, en effet tout élément non nul admet un inverse :

$$x = a + ib \ \Rightarrow\ x^{-1} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = \underbrace{\left(\frac{a}{a^2+b^2}\right)}_{\in\mathbb{Q}} + i\underbrace{\left(\frac{-b}{a^2+b^2}\right)}_{\in\mathbb{Q}}$$